



Oude Waalsdorperweg 63
Postbus 96864
2509 JG Den Haag

www.tno.nl

T 070 374 00 00
F 070 328 09 61
info-DenV@tno.nl

TNO-rapport**TNO-DV1 2005 A153****Testbed omgeving voor gedistribueerde
waarneming**

Datum	mei 2006
Auteur(s)	dr. L.J.H.M. Kester dr. M.G. Maris
Rubricering rapport	Ongerubriceerd
Vastgesteld door	drs. W. Pelt
Vastgesteld d.d.	8 maart 2006
Titel	Ongerubriceerd
Managementuittreksel	Ongerubriceerd
Samenvatting	Ongerubriceerd
Rapporttekst	Ongerubriceerd
Bijlagen	Ongerubriceerd
Exemplaarnummer	9
Oplage	17
Aantal pagina's	34 (incl. bijlage, excl. RDP & distributielijst)
Aantal bijlagen	1

DISTRIBUTION STATEMENT A
Approved for Public Release
Distribution Unlimited

Alle rechten voorbehouden. Niets uit dit rapport mag worden vermenigvuldigd en/of openbaar gemaakt door middel van druk, fotokopie, microfilm of op welke andere wijze dan ook, zonder voorafgaande schriftelijke toestemming van TNO.

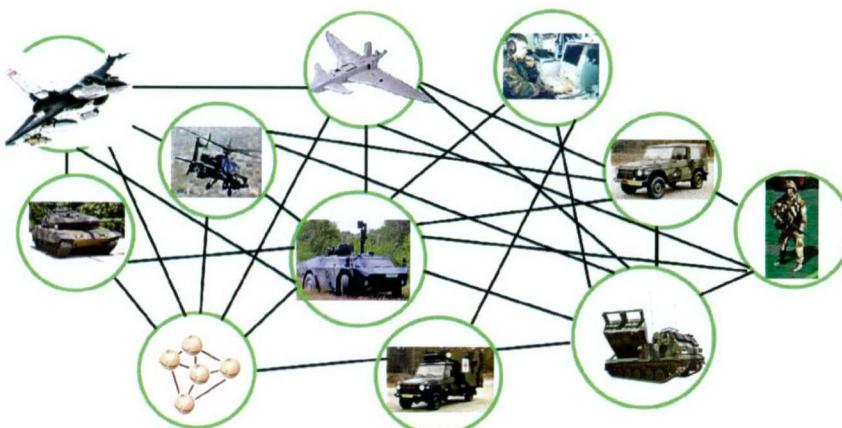
Indien dit rapport in opdracht van het ministerie van Defensie werd uitgebracht, wordt voor de rechten en verplichtingen van de opdrachtgever en opdrachtnemer verwezen naar de 'Modelvoorwaarden voor Onderzoeks- en Ontwikkelingsopdrachten' (MVDT 1997) tussen de minister van Defensie en TNO indien deze op de opdracht van toepassing zijn verklaard dan wel de betreffende ter zake tussen partijen gesloten overeenkomst.

© 2006 TNO

AQ F06-11-9008

Testbed omgeving voor gedistribueerde waarneming

Het optreden van Defensie zal in de toekomst in toenemende mate een netwerk-centrisch karakter hebben. Dit behelst ondermeer de inzet van kleinere modulaire eenheden waarbij de data van verschillende devices, deels geplaatst op onbemande platformen, moet worden samengevoegd tot bruikbare informatie. Dit rapport beschrijft een Testbed omgeving als platform voor zulke samenwerkende devices.



Probleemstelling

Dit projectrapport is onderdeel van het programma V219 en beschrijft een Testbed omgeving waarbinnen sensorcombinaties (eventueel ondersteund door andersoortige randapparatuur) kunnen worden getest en geëvalueerd. Data van verschillende sensoren, deels geplaatst op onbemande platformen, moet kunnen worden samengevoegd tot informatie die door operationele teams gebruikt kan worden. Bij de specificatie van dergelijke complexe systemen is een vroegtijdige afweging van consequenties aangaande de implementatie van kritische componenten, de realiseerbaarheid en de daarmee gepaard gaande kosten van wezenlijk belang.

Beschrijving van de werkzaamheden

In het eerste deel van dit document komen de verschillende concepten waarin gedistribueerde sensoren een rol kunnen spelen alsmede de protocollen van het Testbed aan de orde. Er wordt beschreven hoe ieder apparaat als een 'Networked Intelligent Device' kan worden gezien, hetgeen integratie en samenwerking tussen devices in een netwerk mogelijk maakt. Het tweede deel beschrijft een demonstratie-systeem van een complete compound security applicatie met het Testbed.

Hierbij komen geselecteerde subsystemen

aan bod en hun samenhang in het complete demonstratie-systeem.

Resultaten en conclusies

Er is aangetoond dat data van verschillende sensoren kunnen worden samengevoegd tot bruikbare informatie. Als demonstratie-systeem is gekozen voor het detecteren en volgen van bewegende mensen, waarbij metingen van verschillende sensoren in het volgproces worden gecombineerd.

Tijdens dit project is gebleken, dat informatie-uitwisseling tussen verschillende systemen in een genetwerkte omgeving geenszins triviaal is. De uitdaging zal blijven zitten in het definiëren van de juiste interfaces die aan de ene kant generiek en flexibel zijn en aan de andere kant specifiek en applicatie-afhankelijk zijn.

Toepasbaarheid

Het Testbed is gereed voor gebruik. De omgeving kan gebruikt worden voor het testen en evalueren van multi-device systemen, bijvoorbeeld in het kader van NEC.

PROGRAMMA	PROJECT
Programmabegleider drs. W. Pelt, DMKM/WCS/TV	Projectbegeleider drs. W. Pelt, DMKM/WCS/TV
Programmaleider ing. J.C.P. Bol, TNO Defensie en Veiligheid, Integrated Systems	Projectleider dr. M.G. Maris, Transceivers and real-time signal processing en dr. ir. L.J.H.M. Kester Integrated Systems
Programmatitel Embedded Technieken in Militaire Systemen	Projecttitel Protocollen Testbed Omgeving, en Demonstratie Testbed Omgeving
Programmanummer V219	Projectnummer 015.33721 en 015.34353
Programmaplanning Start 1 januari 2003 Gereed 31 december 2005	Projectplanning Start 1 januari 2004 Gereed 31 december 2005
Frequentie van overleg Met de programma/project begeleider werd 3 maal gesproken over de invulling en de voortgang van het onderzoek.	Projectteam dr. ir L.J.H.M. Kester, dr. M.G. Maris, dr. S.P. van den Broek, ir. Ch. Lievers, ir. R. Lukasse, dr. ir. J.A.A.J. Janssen, dr. J. Bergmans

Contact en rapportinformatie

Oude Waalsdorperweg 63
Postbus 96864
2509 JG Den Haag

T 070 374 00 00
F 070 328 09 61

info-DenV@tno.nl

TNO-rapportnummer
TNO-DV1 2005 A153

Opdrachtnummer
-

Datum
mei 2006

Auteur(s)
dr. L.J.H.M. Kester
dr. M.G. Maris

Rubricering rapport
Ongerubriceerd

Inhoudsopgave

Managementuittreksel.....	2
1 Inleiding.....	5
2 Toepassingen.....	7
2.1 Introductie.....	7
2.2 Compound security.....	8
2.3 Optreden in verstedelijkt gebied.....	8
2.4 Bescherming vloot.....	8
2.5 Scheepsinspecties	9
2.6 Platformmanagement	9
2.7 Object bewaking	10
3 Functionele Beschrijving.....	11
3.1 Inleiding	11
3.2 Networked Intelligent Devices	12
3.3 Communicatie-interface.....	15
3.4 Het onderliggende platform .NET	15
3.5 Lookup service.....	15
3.6 Zoeken naar devices (service discovery)	17
3.7 DeviceML.....	18
3.8 Data-uitwisseling	19
3.9 Samenvattend.....	19
4 Demonstratiesysteem.....	20
4.1 Demonstratiesysteem.....	20
4.2 Radar module.....	21
4.3 Infrarood module	23
4.4 CSD module	24
5 Fusie en Tracking module M6T	26
5.1 Resultaten	28
6 Conclusie.....	30
7 Referenties.....	31
8 Ondertekening.....	32
Bijlage(n)	
A Universal Contact Message format	

1 Inleiding

Het optreden van Defensie zal in de toekomst in toenemende mate een netwerk-centrisch karakter hebben. Ontwikkelingen op dit gebied behelsen de inzet van kleinere modulaire eenheden waarbij de data van verschillende sensoren, deels geplaatst op onbemande platformen, moet worden samengevoegd tot bruikbare informatie. Dit vereist compacte, in real-time werkende systemen met een hier op toegesneden communicatienetwerk.

Voor commando-posten bijvoorbeeld wordt het steeds moeilijker om de juiste beslissingen te nemen zonder adequate ondersteuning van technische hulpmiddelen. Een gedistribueerd waarnemingsysteem is een voorbeeld van een technische ondersteuning. Zo'n systeem bestaat uit een aantal sensoren, mogelijk ook actuatoren waaronder displays, die via een data-communicatienetwerk gekoppeld zijn.

Zulke systemen hebben tot doel de 'situation awareness' van de commando-post te verbeteren. Dit is onder andere van belang voor beveiliging (schepen, compounds), expeditionair optreden en evaluatie van concepten voor Networked Enabled Capabilities (NEC) en autonome systemen.

Ofschoon het concept van gedistribueerde waarneming niet nieuw is, zorgen ontwikkelingen van de afgelopen jaren op technologisch gebied ervoor dat nu praktisch werkbare systemen gecreëerd kunnen worden. De momenteel grootste problemen zijn standaardisatie van de interfaces (zowel op hardware als op software niveau) en de stabiliteit van het complete systeem. Typische voorbeelden van gedistribueerde waarnemingsystemen zijn radars of electro-optische sensoren voor detectie en volgen van objecten ('search, track and trace'). Andere voorbeelden waarbij gedistribueerde waarneming een belangrijke rol kan spelen is bij de detectie en localisatie van snipers of mortieren.

Om informatie van sensoren te combineren wordt vaak gebruik gemaakt van een centraal systeem, dat de signalen van de sensoren inleest, verwerkt en combineert. Doorgaans is het veel en inefficiënt werk om dit voor elkaar te krijgen. Dit komt omdat de interfaces niet gestandaardiseerd zijn noch de data die door de sensoren geleverd wordt. Bovendien zal er, in het geval dat er veel sensoren gebruikt worden, een 'overload' ontstaan bij de centrale van te verwerken data. Een gedistribueerd waarnemingsysteem daarentegen bestaat uit 'intelligente' sensoren die zelf een deel van de informatieverwerking verzorgen voordat ze hun resultaten naar de commando post of naar andere sensoren versturen voor evaluatie. Dit heeft het grote voordeel dat de signaalverwerking verspreid wordt over het netwerk hetgeen gunstig is voor bandbreedte-behoefte omdat de ge-extraheerde informatie-berichten doorgaans kleiner zijn dan de rauwe sensordata. Bovendien zal er geen overload optreden bij de centrale.

Dit projectrapport is onderdeel van het programma V219 en beschrijft een Testbed-omgeving waarbinnen sensorcombinaties (eventueel ondersteund door andersoortige randapparatuur) kunnen worden getest en geëvalueerd. Data van verschillende sensoren, deels geplaatst op onbemande platformen, moet kunnen worden samengevoegd tot informatie die door operationele teams gebruikt kan worden. Bij de specificatie van dergelijke complexe systemen is een vroegtijdige afweging van consequenties aangaande de implementatie van kritische componenten, de realiseerbaarheid en de

daarmee gepaard gaande kosten van wezenlijk belang. Een voorstudie die tot de specificaties van het Testbed hebben geleid is beschreven in [1].

Bovendien bevordert een Testbed omgeving, die in meerdere projecten en programma's gebruikt kan worden, het hergebruik van kennis en technologie-ontwikkelingen en draagt bij tot een betere samenhang tussen de verschillende programma's. Dit maakt het mogelijk om technologieën en ontwikkelingen uit te wisselen tussen verschillende applicatielijnen (bijvoorbeeld van de Koninklijke Marine en Koninklijke Landmacht). Dit alles resulteert in een verbrede kennisbasis met betrekking tot gedistribueerde waarneming.

De doelstellingen van het Testbed zijn:

- 1 Efficiënter onderzoek en ontwikkeling van concepten en technologieën door hergebruik van infrastructuur (het Testbed).
- 2 Demonstratie van de relevantie van nieuwe technieken en applicaties ten behoeve van defensie.
- 3 Evaluatie van concepten en technieken als onderdeel van een hybride (simulatie-demonstratie) omgeving.
- 4 Kennisopbouw met betrekking tot gedistribueerde waarnemingssystemen ten behoeve van consultancy aan de Krijgsmacht en realistische simulatie van dergelijke systemen.

Dit document is onderverdeeld in twee delen, die de werkzaamheden beschrijven van twee samenhangende projecten, namelijk 'Protocollen Testbedomgeving' en 'Demonstratie Testbedomgeving'. Het eerste deel beschrijft het Testbed en de gebruikte protocollen, in hoofdstuk 2 en 3. Als basis voor de gemaakte keuzes gelden de aanbevelingen uit het voorafgaande project 'Definitie Testbed Omgeving' [1]. Het tweede deel beschrijft een demonstratie-systeem van een complete applicatie met het Testbed. Dit werk is het resultaat van project 'Demonstratie Testbedomgeving'. Hierin komen een aantal geselecteerde sensoren aan bod en hun samenhang in een compleet systeem voor gedistribueerde waarneming wordt gedemonstreerd. Tot slot volgen de conclusies in het laatste hoofdstuk.

2 Toepassingen

Het primaire doel van de Testbed omgeving is het testen en evalueren van gedistribueerde waarnemingssystemen. In dit hoofdstuk wordt ingegaan op een aantal mogelijke toepassingen van dit testbed.

2.1 Introductie

De Nederlandse Krijgsmacht richt zijn activiteiten dikwijls op vredesoperaties. Tijdens deze operaties heeft de bescherming van eigen personeel en materieel een hoge prioriteit. In dit verband is er behoefte aan systemen die een grote flexibiliteit bezitten qua reactie op de lokaal heersende dreiging en die bovendien de minimale bezetting van personeel vereisen. De motivatie voor deze behoefte is hieronder samengevat in een aantal huidige knelpunten met betrekking tot het gebruik van technische ondersteuningssystemen:

- Hoge personele inzet.
- Risico's voor het personeel.
- Beperkte dekkingsgraad.
- Extreme omgevingsfactoren zoals hitte, kou, mist, zandstormen, etc.
- Niet altijd wenselijke militaire zichtbaarheid terwijl de omgeving toch geobserveerd moet worden.
- Omgang met onverwachte incidenten.
- Onbekendheid met de situatie.

Het gebruik van een gedistribueerd sensorsysteem kan tegemoet komen aan deze knelpunten. Door gebruik te maken van autonome sensoren is minder personeel nodig voor bewaking en observatie. De observatie vindt plaats op afstand, dit reduceert het risico voor het personeel. Door de inzet van sensoren in combinatie met het personeel worden meer observatiepunten verkregen en wordt de dekkingsgraad groter.

Met andere woorden met dezelfde hoeveelheid personeel kan een groter gebied worden gecontroleerd. Daarnaast zijn sensoren altijd waakzaam en kunnen relatief risicolos fungeren als vooruitgeschoven observatieposten waardoor een vroegtijdige alarmering wordt verkregen en het gevaar voor overmacht wordt gereduceerd. Daarnaast geeft de inzet van sensoren een completer beeld van de momentane situatie door de hoeveelheid observatiepunten. Door het gebruik van digitale kaarten worden de actuele troepen-, burger- en voertuigverplaatsingen real-time in kaart gebracht. Dergelijke sensoren kunnen bijvoorbeeld voor een snelle inzet worden uitgestrooid waarna de sensoren autonoom bepalen welke sensor welke informatie verzamelt en van welk gebied. Dit met als doel het optimaliseren van het energieverbruik (en dus de levensduur) bij een zo goed mogelijke dekkingsgraad. De dekkingsgraad kan bijvoorbeeld worden bepaald door het uitwisselen van de GPS posities tussen de sensoren.

In het veld kunnen een groot aantal verschillende sensoren worden ingezet.

Hierbij kan gedacht worden aan:

- Lichtstraal onderbrekers.
- Struikeldraad.
- Bewegingsdetectie met radar of infrarood.
- Snelheidsmeting met radar.
- Objectdetectie en classificatie met radar of infrarood.
- Seismische sensoren (bijvoorbeeld voetstapdetectors).

- Magnetische lussen.
- Akoestische sensoren.
- Strijdgasdetectoren.
- Meteorologische stations.

In de volgende paragrafen worden een aantal typische applicaties beschreven waarin gedistribueerde intelligentie een belangrijke rol kan spelen.

2.2 Compound security

Wanneer een militaire eenheid ergens neerstrijkt moet het kampement (compound) beschermd worden tegen indringers. Wenselijk is het dat het terrein om de compound zo snel mogelijk na vestiging bewaakt wordt. Verschillende methoden zijn denkbaar hiervoor. Momenteel worden hiervoor bijvoorbeeld gevechtsveld-radar, warmtebeeld-cameras of tripwires gebruikt. Deze systemen staan doorgaans op zichzelf, dat wil zeggen, ze zijn niet op een data-netwerk aangesloten. Momenteel is er echter behoefte aan systemen die wel opgenomen kunnen worden in een netwerk, zodat een grotere flexibiliteit met betrekking tot hun inzet verkregen wordt en tegelijkertijd een gereduceerde bezetting van personeel mogelijk is, omdat de sensoren niet meer handmatig uitgelezen hoeven te worden.

Gebruik van gedistribueerde sensoren in een samenhangend netwerk is een veelbelovende aanpak om compounds beter te helpen beveiligen. In de afgelopen jaren zijn al verschillende onderzoeksopdrachten uitgevoerd, die gericht waren op detectie van bewegende objecten in een ruimte. Doorgaans werd een bepaald type sensor gebruikt tijdens deze studies, dus bijvoorbeeld uitsluitend radar of infrarood of daglicht camera's. Zo heeft TNO in 2003 de mogelijkheden bestudeerd om met zeer kleine en gedistribueerde sensoren het gebied rondom een compound te bewaken.

De bevindingen van dit onderzoek zijn beschreven in [2]. Een implementatie van dit systeem met een groot aantal sensoren werd gedaan binnen het project SOWnet, ook binnen dit programma V219. Deze maakt gebruik van bewegingsmelders om objecten rondom de compound waar te nemen.

2.3 Optreden in verstedelijkt gebied

Bij sommige operaties zal het Nederlandse leger te maken hebben met optreden in verstedelijkte gebieden. Dit betekent dat er in een dorp of een stad verkennings- en patrouille taken te verrichten zijn die vaak in gevaarlijke gebieden gelegen zijn. Om het risico voor het militaire personeel te minimaliseren en toch een goede presentie te behouden kan er gebruik gemaakt worden van semi-autonome robotsystemen. Zulke robots worden op afstand bestuurd en kunnen enkele taken zelfstandig uitvoeren (bijvoorbeeld obstakels ontwijken of detectie van interessante gebeurtenissen). Een combinatie van een aantal robots en (uitgestrooide) sensoren kunnen de detectie- en observatie-mogelijkheden nog verder vergroten.

2.4 Bescherming vloot

Marineschepen in (buitenlandse) havens zijn kwetsbaar tegen terroristische aanslagen. Denk bijvoorbeeld aan de USS Cole waar met behulp van een rubberbootje verschillende compartimenten zijn vernietigd en marinpersoneel is gedood. Het gebruik van een early warning system kan in deze gevallen uitkomst bieden.

Hierbij valt te denken aan sensoren op het schip, rondom het schip in het water, maar ook op de kade. De opzet van een dergelijk sensor netwerk moet zodanig zijn dat een sensor die stuk gaat direct vervangen kan worden door een werkend exemplaar.

De methode van communicatie moet gestandaardiseerd zijn zodat ook nieuwe sensoren eenvoudig kunnen worden toegevoegd. Door de aanwezigheid van lokale intelligentie zijn de sensoren in staat om problemen met de communicatie (bijvoorbeeld te veel zenders, jamming, et cetera) op te vangen. Mogelijke oplossingen zijn: automatische hertransmissie, het zoeken van een ander communicatie pad of het opslaan van gegevens en deze later versturen als deze tegen de tijd van herstelde communicatie nog actueel zijn. Een mogelijk nadeel van sensoren is de false alarm rate. Deze kan echter worden verlaagd door de detecties van een aantal sensoren te combineren.

Bijvoorbeeld een bewegingsmelder, sonar en een camera, of een radar die zijn meting kalibreert met het in het netwerk aanwezige meteorologisch station. Door de reductie van false alarms wordt de operator minder belast en raakt minder vermoed waardoor deze alerter is op verdachte situaties. Dergelijk snel in te zetten in dringerdetectiesystemen zijn ook te gebruiken in (civiele) havens om goederen te bewaken.

2.5 Scheepsinspecties

Een belangrijke taak in vredesoperaties is het inspecteren van schepen. Een systeem dat hierbij behulpzaam kan zijn is een combinatie van sensoren zoals satellieten, radarsystemen aan land en op schepen, en een netwerk van intelligente boeien.

Het combineren van de informatie afkomstig van deze waarnemingssystemen kan leiden tot het detecteren en onderscheppen van schepen die verdachte routes varen (bijvoorbeeld rondjes varen maar geen havens aandoen).

2.6 Platformmanagement

Om calamiteiten op marine schepen adequaat en snel het hoofd te bieden onderzoekt TNO automatiseringsconcepten gebaseerd op gedistribueerde systemen [8].

Deze systemen monitoren met behulp van sensoren de technische werking van een scheepsplatform en corrigeren indien nodig autonoom ongewenste situaties.

Voorbeeld van systemen die op deze wijze gemaakt kunnen worden zijn onder andere: opwekking en verdeling van elektriciteit, opwekking en verdeling van koudwater, opwekking en verdeling van brandbluswater, opwekking en verdeling van hogedruk- en lagedrukluft, aangeven evacuatie of beschikbare routes in het schip, et cetera.

Robuustheid van een dergelijk platform-managementsysteem kan gerealiseerd worden door de autonome (bewaking en controle) functies zoveel mogelijk te verdelen over het schip. Wanneer een deel van het systeem uitvalt blijven bepaalde kritische functies locaal functioneren (bijvoorbeeld pompen inschakelen, ruimtes afsluiten, et cetera) waardoor het systeem onafhankelijk wordt van een centrale besturing. Dit vereist een systeembenedering die in staat is om met deze 'distributie van intelligentie' om te gaan. Dit principe wordt in het project 'Robuuste Automatisering' (programma Toekomstige Platformen, V048) onderzocht door TNO voor het koudwatersysteem uit de hoofdfunctie Support SEWACO (Sensoren-, Wapen- en Commandosystemen).

Het koudwatersysteem heeft als taak het opwekken en verdelen van koud water.

Het koudwatersysteem loopt door een groot deel van het schip. De correcte werking wordt gemonitord d.m.v. sensoren met lokale intelligentie. In geval van een calamiteit (lekkages, ongebalanceerde koeling, et cetera) wordt met behulp van actuatoren (kleppen, cross-overs, pompen, et cetera) het systeem gereconfigureerd zodat de SEWACO apparatuur een hogere graad van beschikbaarheid heeft zonder dat een

operator nodig is waardoor een hoge reactiesnelheid gewaarborgd is. Een dergelijke oplossing vereist onder andere: sensoren en actuatoren op verschillende locaties op het schip, lokale intelligentie om uitval van sensoren te compenseren door andere routes te genereren en een robuust netwerk voor de communicatie tussen de sensoren en actuatoren.

2.7 Object bewaking

In veel gevallen is het gewenst dat (militair) materieel bewaakt wordt. Als bijvoorbeeld een helikopter op een vliegveld geland is, dan dient deze voortdurend bewaakt te worden, dag en nacht. Hier kunnen genetwerkte sensoren een belangrijke rol vervullen. Bewegings-detectoren en (infrarood) camera's kunnen rondom het te bewaken object gezet worden. Zodra beweging wordt waargenomen in de buurt van het object zal de bewaker, die op een andere plaats kan zitten, geïnformeerd worden. Deze vorm van bewaking is veel trefzekerder dan alleen visuele inspectie. Bovendien kan op deze wijze één bewaker meerdere objecten tegelijkertijd bewaken.

3 Functionele Beschrijving

De doelstelling van het Testbed is om de functionele mogelijkheden van interoperabele devices te demonstreren. Dit is echter alleen mogelijk indien het Testbed beschikt over gestandaardiseerde protocollen voor data- en informatie uitwisseling tussen de verschillende onderdelen van het Testbed. Deze protocollen worden in dit hoofdstuk beschreven.

3.1 Inleiding

De bedoeling van het Testbed is om een platform te creëren dat gebruikt kan worden om systeemconcepten op het gebied van gedistribueerde waarneming te evalueren. In principe komt het er op neer dat verschillende systemen (sensoren en/of actuatoren) met elkaar moeten kunnen ‘samenwerken’ om een meerwaarde te leveren aan de kwaliteit van de waarnemingen. Het Testbed zal dus een infrastructuur moeten leveren die data van verschillende soorten sensoren kan uitlezen en ook actuatoren kan aansturen. We spreken hier dus over een ‘system of systems’ (tegenwoordig ook wel ‘system of platforms’ genoemd). Bovendien zal het Testbed in staat moeten zijn om data van sensoren te fuseren en te evalueren.

Zo’n gewenste infrastructuur kan alleen tot stand komen als er een aantal functies gestandaardiseerd zijn, te weten:

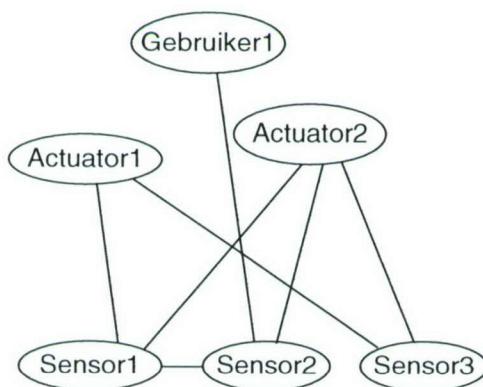
- 1 *Netwerk.* Apparaten zijn alleen bruikbaar als ze een netwerkaansluiting bezitten voor een bepaald netwerkprotocol.
- 2 *Communicatie-interface.* Om data uit te lezen en apparatuur aan te sturen moet er een communicatie-protocol zijn voor het uitwisselen van berichten. Zonder standaard protocol is samenwerking niet mogelijk. Dit kan vergeleken worden met de syntax of grammatica van een taal.
- 3 *Data-interpretatie.* Als het netwerk draait en er data verzonden kan worden, dan moet de data nog geïnterpreteerd worden. Als hier geen afspraken over gemaakt zijn dan begrijpen ze elkaar niet (de apparaten moeten allen dezelfde ‘taal spreken’). Dit kan vergeleken worden met de semantiek of betekenis van woorden in een taal.

Wat betreft het netwerk: de meeste apparaten met een netwerk-interface zullen een gangbare standaard kiezen, zoals ethernet met TCP/IP, Bluetooth of GPRS. Dit is dus geen probleem voor integratie in het Testbed dat in principe al deze protocollen kan afhandelen.

Lastiger wordt het doorgaans bij het vaststellen van wat er over het netwerk gestuurd wordt per apparaat. Zelfs als het netwerk ethernet is met 100Mbits/s en het netwerk-protocol TCP/IP, dan is nog steeds niet bekend hoe een gebruiker data uit dat apparaat (een sensor) kan krijgen en hoe die vervolgens te interpreteren. Vaak wordt bij ieder apparaat een communicatie-protocol meegeleverd waarin staat op welke manier bepaalde parameters ingesteld moeten om data te kunnen lezen. De data wordt dan in een bepaald formaat geleverd dat vaak heel specifiek is voor dat apparaat. Er is dus vaak geen standaard, noch voor het communicatie-protocol noch voor het data-protocol. Dit probleem kan worden ondervangen door te proberen deze interfacing te standaardiseren. In de volgende paragraaf wordt een methode geïntroduceerd om dit te realiseren

3.2 Networked Intelligent Devices

Een typische Testbed-applicatie bestaat uit een aantal sensoren, actuatoren en gebruikers die informatie uitwisselen via een netwerk. Een sensor kan worden beschreven als een instrument dat in staat is om een fenomeen te observeren en deze te vertalen in een getal of een verzameling getallen. Een actuator is een instrument dat in staat is om zijn omgeving te beïnvloeden. Een controller device kan, via een operator of autonoom, acties ondernemen om de werking van de applicatie te beïnvloeden. Ook de interactie met de gebruiker is een taak voor een controller device: de gebruiker kan commando's geven of informatie aflezen. In dit verband wordt de term NID (Networked Intelligent Device) gebruikt voor elk apparaat (sensor, actuator of controller (gebruiker)) dat onderdeel uitmaakt van het netwerk. Figuur 3.1 toont een principe-schema van een Testbed-systeem. Elke ovaal in deze figuur is een soort NID. Er zijn dus sensor-NIDs, actuator-NIDs en gebruiker-NIDs.



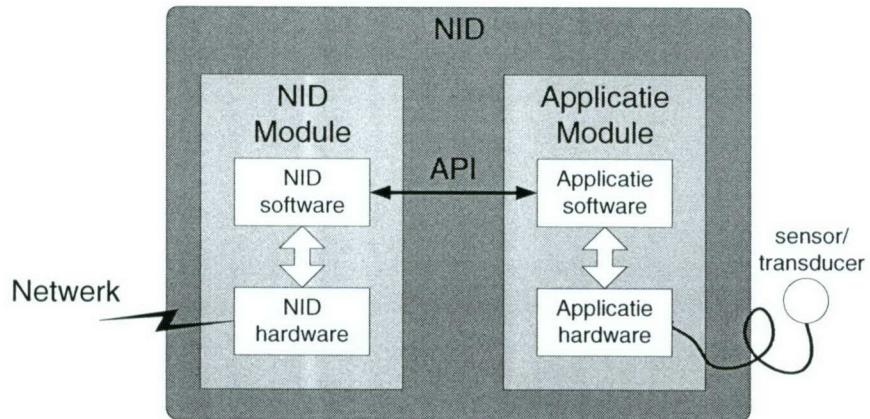
Figuur 3.1 Principe-schema van een typische Testbed-toepassing.

De NIDs delen informatie via het datanetwerk. De sensoren (bijvoorbeeld radar of electro-optisch) observeren de omgeving terwijl de actuatoren (bijvoorbeeld jammers) gebaseerd op de sensorinformatie de omgeving manipuleren. Met behulp van beeldschermen wordt de verkregen informatie zichtbaar gemaakt aan de gebruiker die vervolgens eventueel actie kan ondernemen.

Een NID bevat functies met betrekking tot het Testbed en functies met betrekking tot de applicatie die gebruik maakt van de Testbed omgeving. Om te komen tot een goede definitie van het Testbed is het belangrijk om een onderscheid te maken tussen de functies van het Testbed zelf en de applicaties die gebruik maken van het Testbed. Daarom onderscheiden we twee modules:

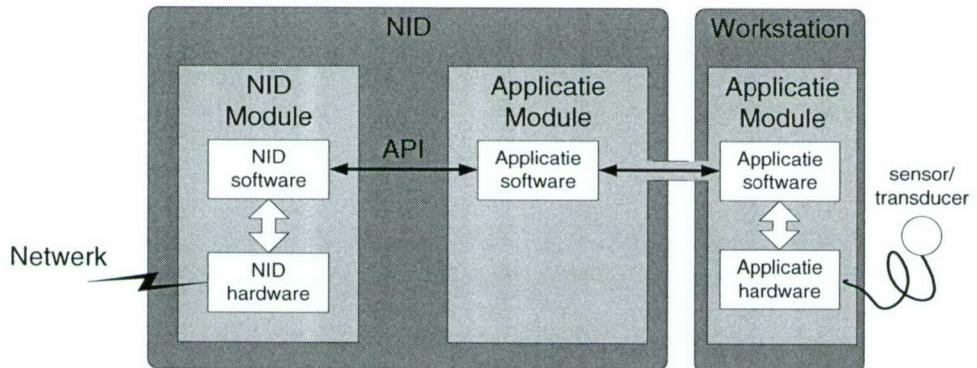
- 1 De NID Module.
- 2 De Applicatie Module.

Deze scheiding in modules is weergegeven in figuur 3.2. Elke module kan op zijn beurt weer opgesplitst zijn in andere modules. De NID Module vormt de verbinding met het netwerk en levert diensten aan de Applicatie Module. De Applicatie Module bevat de applicatie-software (signaalverwerking en dergelijke). Om ervoor te zorgen dat beide modules goed op elkaar aansluiten en dat de applicatie-ontwikkelaar exact weet hoe de applicatie kan worden getest op het Testbed wordt gebruik gemaakt van een API (Application Program Interface), die de applicatie-ontwikkelaar gemakkelijk toegang verschafft tot de functionaliteiten van de NID-module.



Figuur 3.2 Modules binnen een NID.

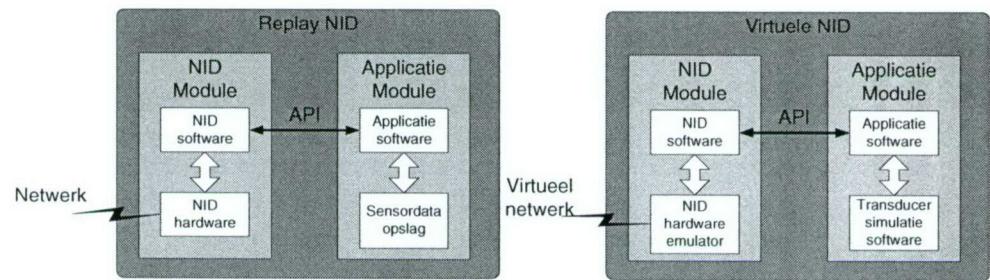
Voor specifieke applicaties kan het voorkomen dat de resources (rekenkracht, geheugen, et cetera) van de NID niet toereikend zijn. In dergelijke gevallen kan de applicatie ontwikkelaar natuurlijk ook gebruik maken van een eigen workstation met daaraan de sensor. Dit workstation communiceert vervolgens zijn bevindingen naar de NID module, zie figuur 3.3. De wijze van communicatie tussen het workstation en het device valt volledig onder de verantwoording van de applicatie ontwikkelaar. Daarnaast is het natuurlijk ook mogelijk dat de applicatie ontwikkelaar het workstation direct aansluit op het netwerk waarbij de NID module op het workstation wordt geïmplementeerd.



Figuur 3.3 Uitbreiding van de Applicatie Module als een NID zelf onvoldoende resources heeft zoals rekenkracht, geheugen of als de sensorinterface niet voldoet.

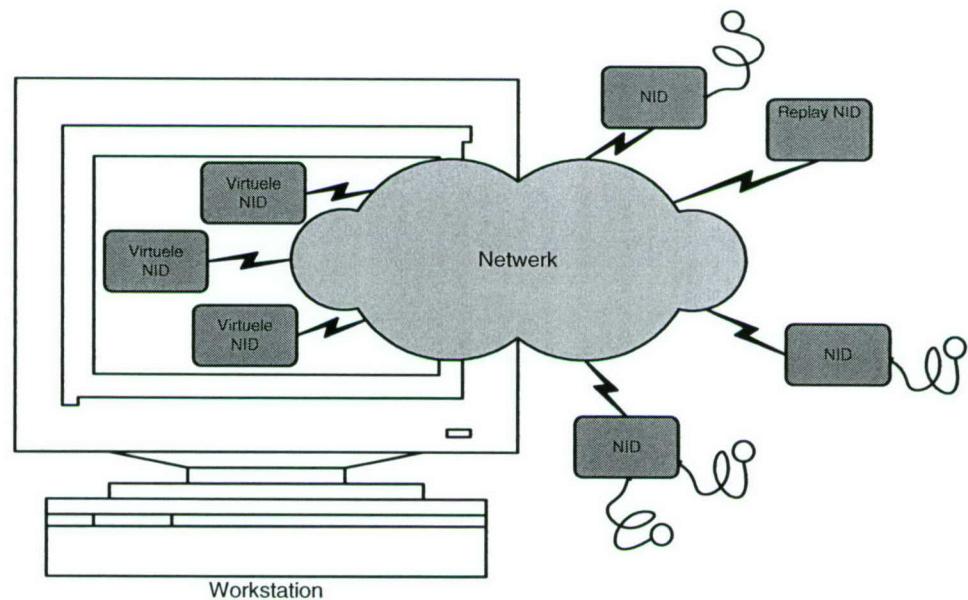
Door de API eenduidig te specificeren hoeft de applicatie ontwikkelaar geen kennis te hebben van de wijze van communicatie over het netwerk. Dit wordt immers verzorgd door de NID module. Door deze scheiding kan in principe elk type netwerk met bijbehorende protocollen worden gebruikt binnen de Testbed Omgeving zonder dat de Applicatie Module hoeft te worden aangepast.

In sommige situaties is het niet praktisch of realiserbaar om de fysieke meting met het Testbed uit te voeren. Bijvoorbeeld omdat de meetdata afkomstig is van de sensoren van een operationeel scheepsplatform of omdat het wenselijk is om een specifiek scenario te testen. In deze situaties is het wenselijk om de opgenomen meetdata 'af te spelen' in het Testbed. Voor dergelijke situaties kan gebruik worden gemaakt van *replay NIDs*. In deze NIDs bestaat de Applicatie Module alleen uit software en is er dus geen sensor of actuator, zie figuur 3.4. De software simuleert de aanwezigheid van de sensor of actuator.



Figuur 3.4 De modules in een replay NID en een virtuele NID.

Een stap verder is het emuleren van de gehele NID in software d.m.v. een virtuele NID (zie figuur 3.4). Hiermee is het zelfs mogelijk om een deel van het netwerk te simuleren op bijvoorbeeld een werkstation. Een test applicatie bestaat dan uit een virtueel netwerk met virtuele NIDs en een fysiek netwerk met fysieke devices en/of replay NIDs. Dit is gevisualiseerd in figuur 3.5.



Figuur 3.5 Combinatie van virtuele NIDs, replay NIDs en NIDs.

In de volgende paragrafen wordt beschreven hoe de NIDs gebruikt kunnen worden om de interfacing tussen apparaten te standaardiseren.

3.3 Communicatie-interface

Het Testbed is opgebouwd uit een netwerkinfrastructuur dat gebruik maakt van de '.NET' omgeving van Microsoft. Devices kunnen zich aanmelden met behulp van een XML-file conform het DeviceML-schema protocol (zie §3.7). De devices vinden elkaar op het netwerk door een 'service request' naar een lookup service te sturen. Nadat NIDs elkaar gevonden hebben kunnen ze communiceren door zgn. UCM berichten uit te wisselen. Hieronder worden deze functies nader uitgelegd.

3.4 Het onderliggende platform .NET

Voor de implementatie van het Testbed is gekozen voor de .NET omgeving. Dit is een software platform van Microsoft dat uitermate geschikt voor het opzetten van het Testbed omdat er een uitgebreide ondersteuning aanwezig is van software-bibliotheken voor netwerkfuncties. Hierdoor kunnen er snel gedistribueerde data-netwerken opgezet worden om gedistribueerde waarnemingsconcepten te testen.

Bovendien is .NET zeer geschikt om met XML te werken. Dit is zeer gunstig omdat het Testbed veelvuldig van XML gebruik maakt, zoals bij de aanmeldingen van de devices (DeviceML), bij Service Discovery en bij de data-uitwisseling. Alleen binnen een NID, dat in feite ook uit verschillende programma's bestaat, wordt geen gebruik gemaakt van XML.

Een nadeel van de .NET omgeving is wel, dat elk device over een behoorlijk grote capaciteit (geheugen en processorkracht) moet beschikken om de onderliggende .NET infrastructuur te kunnen ondersteunen; minimaal een Pentium II is nodig.

Op dit moment draait .NET uitsluitend op Microsoft Windows, hetgeen niet overeenkomstig de oorspronkelijke doelstelling van het Testbed is om verschillende platformen te ondersteunen [1]. Met name het wijdverbreide Linux dient ondersteund te worden. Gelukkig wordt er momenteel ook een .NET versie voor Linux ontwikkeld waar binnenkort gebruik van gemaakt kan worden.

3.5 Lookup service

Binnen een gedistribueerd waarnemingsysteem wordt data tussen NIDs gecommuniceerd, met als doel om door de combinatie van de verschillende observaties een betere en betrouwbaardere detectie, classificatie of identificatie te verkrijgen van de gedetecteerd objecten.

Voordat dit communicatieproces op gang kan komen moeten de NIDs elkaar op het netwerk gevonden hebben. Een goede aanpak is om gebruik te maken van een soort lijst die de eigenschappen van alle NIDs bijhoudt. Deze lijst kan gelezen worden door alle NIDs in het netwerk. Zodra nu een NID een typische functionaliteit wenst dan kan hij die bij de lijst opvragen en, indien aanwezig, krijgt hij referenties naar die NID(s) terug die de gewenste functionaliteit kunnen bieden. Deze faciliteit wordt aangeboden door de 'LookUp Service' (LUS). Het bijbehorende zoekproces heet 'Service Discovery'. Bij de LUS staan dus de eigenschappen van alle NIDs in het netwerk. De eigenschappen zijn weergegeven door middel van DeviceML beschrijvingen (zie paragraaf 3.7).

Dit proces kan worden ge-illustreerd met een voorbeeld. Stel dat een gebruiker de taak heeft om bewegende objecten op een veld waar te nemen. Hierbij wil hij gebruik maken van gedistribueerde waarneming. Hij installeert twee sensortypes die de waarneming moeten verzorgen, te weten een radarsysteem en een infrarood camera. Deze twee systemen zijn in feite NIDs. Deze melden zich op het netwerk aan.

Om nu gedistribueerde waarneming te kunnen plegen moet de data van die sensoren samengevoegd worden. Dit gebeurt bij een derde NID in het netwerk, de 'fusie-NID'. Deze laatste zoekt op het netwerk naar NIDs die bewegende objecten kunnen detecteren. Hij zend hiervoor een verzoek naar de LUS om alle data van NIDs te mogen ontvangen die de service 'bewegende objecten' aanbieden. Na ontvangst van een verbinding naar elk van deze NIDs, kan hij ze contacteren. In dit voorbeeld zijn dat de infrarood-sensor-NID en de radar-NID. Hierna bestaat er een verbinding tussen de fusie-NID en de beide sensor-NIDs. Nu kan datafusie, om objecten te detecteren met gedistribueerde sensoren, op de fusie-NID plaatsvinden door de data van de beide NIDs te combineren. Dit lijkt een ingewikkelde procedure voor slechts twee sensoren. Echter in een omvangrijk systeem met veel verschillende sensoren en services, is deze aanpak zeer gewenst.

De Lookup service heeft dus een centrale rol binnen het Testbed. Bij de LUS staan alle (actieve) devices geregistreerd en geldt als een soort 'gouden gids' voor alle NIDs in het netwerk. Hieronder wordt het proces van aanmelding door NIDs (ook wel 'join genoemd') en het zoeken naar functies van andere NIDs ('service discovery') stapsgewijs beschreven.

3.5.1 Aanmelden/registreren van NIDs (join)

Zodra een NID bij het netwerk dient te worden aangesloten wordt deze procedure gevolgd:

- de LUS luistert op een groep-adres (op port: 11000) naar UDP berichten voor eventuele NID-aanmeldingen;
- de NID start op en stuurt een UDP bericht. Dit bericht is in XML beschreven en heeft de vorm:

```
<?xml version="1.0"?>
<Config>
  <Startup>
    <OwnAddress>10.0.0.11</OwnAddress>
    <ContactPort>11012</ContactPort>
    <InitialDataFile>init_data.xml</InitialDataFile>
  </Startup>
  <GetCSDInfo>
    <CSDPort>10000</CSDPort>
  </GetCSDInfo>
  <GetDeviceMLInfo>
    <DeviceMLPort>11011</DeviceMLPort>
    <DeviceMLFile>CSD.xml</DeviceMLFile>
  </GetDeviceMLInfo>
</Config>
```

Figuur 3.6 Het formaat van het UDP-bericht dat een NID naar de LUS stuurt voor aanmelding. De LUS kan hieruit het IP-adres en portnummer van de NID halen. Ook de naam van de XML-file om de NID te beschrijven staat hierin vermeld (in dit geval 'CSD.xml') in DeviceML formaat. Dit wordt door de LUS opgehaald en in zijn lijst van NIDs geplaatst.

- Na ontvangst van een bericht van een NID wordt het IP-adres van de NID uit het bericht geëxtraheerd.
- Vervolgens wordt het NID IP-adres gebruikt door de LUS om de DeviceML beschrijving van de NID op te halen. Dit wordt gedaan door een TCP/IP verbinding op te zetten tussen de LUS en de NID (via de DeviceML port).
- De DeviceML beschrijving wordt dan gevalideerd door de LUS.
- Als de DeviceML beschrijving correct is, dan wordt deze opgenomen in de actieve sensorenlijst van de LUS.
- Als de DeviceML beschrijving niet correct is, dan wordt deze geweigerd door de LUS en een bericht wordt verstuurd naar de NID. Dit bericht wordt afgevangen door de NID en een bericht naar de (menselijke) eigenaar ervan wordt verstuurd.

3.6 Zoeken naar devices (service discovery)

Zodra een NID een gewenste functionaliteit zoekt (zoals bijvoorbeeld een infrarood-camera die object-informatie kan aanleveren) worden de volgende stappen doorlopen:

- De LUS luistert voortdurend naar berichten van al geregistreerde NIDs (op port 11001).
- NIDs zoeken bij de LUS naar bepaalde functionaliteiten geleverd door andere NIDs. Ze doen dit door een bepaalde beschrijving naar de LUS toe te sturen (via TCP/IP). Zo'n beschrijving heeft de vorm:

```
<?xml version="1.0"?>
<Sensor>
  <IdentifiedAs>
    <TypeOfSensor>radar</TypeOfSensor>
  </IdentifiedAs>
</Sensor>
```

Figuur 3.7 Voorbeeld van een zoekopdracht voor een sensor van het type ‘radar’. De vragende NID stuurt dit bericht naar de LUS. Mogelijke types zijn gedefinieerd in DeviceML.

- Vervolgens zal de LUS in de actuele deviceslijst controleren welke NIDs voldoen aan het verzoek en een lijst terugsturen met daarin het IP-adres van de NIDs die voldoen aan de beschrijving.
- De vragende NID kan nu via de verkregen IP-adres(sen) contact leggen met de NIDs die de gewenste dienst kunnen bieden.

3.6.1 Up-to-date houden van de aanmeldingen (leasing)

De LUS elimineert na verloop van tijd zelf oude aanmeldingen van de lijst omdat de bijbehorende NIDs niet meer bereikbaar zijn, bijvoorbeeld omdat deze buiten zendbereik, uitgeschakeld of defect zijn. Een NID is er zelf verantwoordelijk voor dat zijn aanmelding regelmatig wordt hernieuwd indien deze zijn aanmelding wil behouden. De NID stuurt daarom regelmatig een ‘heartbeat’ signaal naar de LUS.

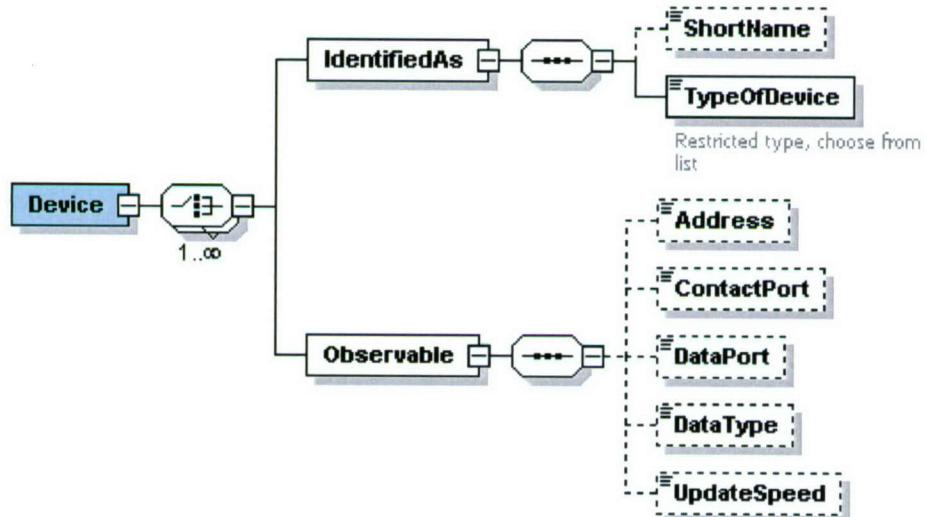
Als de LUS van een NID een aantal seconden geen heartbeat heeft ontvangen dan wordt deze verwijderd uit de lijst.

3.7 DeviceML

Na aanmelding van een NID haalt de LUS de DeviceML beschrijving ervan op. Vanwege de complexiteit en kostbaarheid om standaarden in-huis te ontwikkelen, is ervoor gekozen om gebruik te maken van de concepten die ontwikkeld worden binnen het *sensor web enablement program* (SWEP) [3] van het Open GIS consortium (OGC) [4]. Dit programma binnen het OGC heeft als doelstelling te komen tot een open platform voor het gebruiken van 'web-enabled sensors'. SensorML [5] en Observations and Measurements (O&M) [6] zijn hieruit ontstaan. Deze zijn gerelateerd aan aardobservatiesystemen.

Echter, deze standaarden zijn te ruim opgezet en te complex samengesteld om direct gebruikt te kunnen worden in het Testbed. Een ander nadeel ervan is dat ze uitsluitend geschikt zijn om sensoren te beschrijven en dus geen actuatoren. Dat betekent dat er geen controle-berichten met deze protocollen gedefinieerd kunnen worden. Bovendien zijn deze standaarden nog in ontwikkeling.

Vandaar dat er besloten is om voor het Testbed een ietwat afwijkend protocol te definiëren, gestoeld op de ideeën vanuit SensorML en O&M. Dit protocol hebben we 'DeviceML' genoemd. Dit is een generieke beschrijving voor elk device dat in het Testbed opgenomen dient te worden. In XML heet zo'n omschrijving een 'schema'. DeviceML is geschikt voor alle devices, het is simpel en doeltreffend in zijn opzet en geschikt voor de doelstellingen van het Testbed. In figuur 3.8 is het XML-schema weergegeven.



Figuur 3.8 DeviceML schema voor de Testbed omgeving.

Gebruik makend van DeviceML kan een device gedefinieerd worden met behulp van een XML-file die conform dit formaat geconstrueerd is. In figuur 3.9 staat een voorbeeld van zo'n XML file voor een radar sensor.

```

<?xml version="1.0" encoding="UTF-8"?>
<Device>
  <IdentifiedAs>
    <shortName>Radar sensor</shortName>
    <TypeOfDevice>radar</TypeOfDevice>
  </IdentifiedAs>
  <Observable>
    <Address>10.0.0.11</Address>
    <ContactPort>11033</ContactPort>
    <DataPort>11032</DataPort>
    <DataType>UCM</DataType>
    <UpdateSpeed>1000</UpdateSpeed>
  </Observable>
</Device>

```

Figuur 3.9 Voorbeeld van een XML file voor een radar sensor, gebaseerd op de DeviceML schema beschrijving uit Figuur 3.8.

3.8 Data-uitwisseling

Het uitwisselen van data tussen de NIDs kan plaatsvinden nadat ze elkaar hebben gevonden en een verbinding hebben gecreëerd op de ContactPort (zie figuur 3.9). Het data-formaat dat voor het Testbed is gekozen is een formaat dat door TNO reeds gebruikt werd om ‘tracks’ van waarnemingen vast te leggen. Dit formaat is ‘Universal Contact Message’ (UCM) genoemd. Dit formaat is gedefinieerd als weergegeven in tabel 2.1 (zie ook Bijlage A).

Tabel 3.1 UCM formaat.

field	format	description
big/little endian identifier	U4 ¹	always contains number 0x12345678
sensor id	U4	unique sensor number for specific measurement setup
message id	U4	serial number for blocks of contacts from one sensor, for each sensor this number starts with 1
number of contacts	U4	number of contacts in message
header format id	U4	header format number
contact format id	U4	contact format number

¹ U4 means unsigned integer of 4 bytes

3.9 Samenvattend

Hiermee is de functionaliteit van het Testbed beschreven. Ieder device (NID) dat aangesloten dient te worden op deze omgeving wordt omschreven met de gestandaardiseerde XML-beschrijving (DeviceML), zodat communicatie tussen devices, en de rest van het netwerk, gegarandeerd is. Daarna vind data-communicatie plaats over de ContactPort in het UCM-formaat. In de volgende hoofdstukken wordt een scenario en demonstratiesysteem beschreven dat van dit Testbed gebruik maakt.

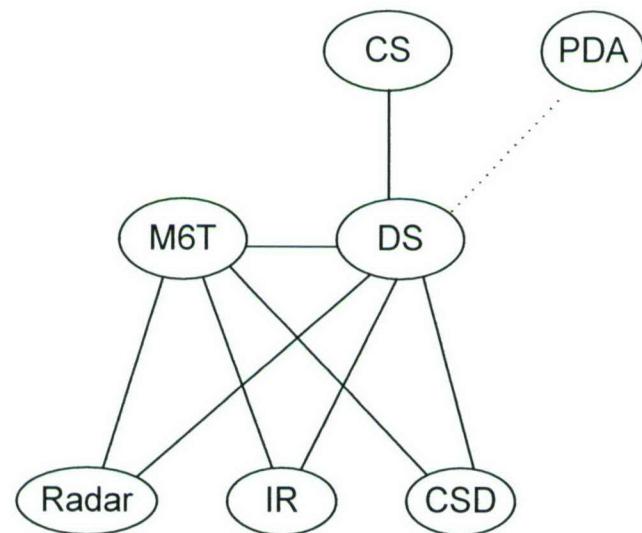
4 Demonstratiesysteem

De hier beschreven applicatie demonstreert een bewakingsysteem dat in een compound-beveiligingsysteem gebruikt zou kunnen worden. De taak van het systeem is de detectie van bewegende objecten en het tracken van deze objecten met verschillende soorten sensoren. De objecten zijn bijvoorbeeld insluipers in het gebied rondom de compound. De gekozen sensoren zijn radar, infrarood en bewegingsmelders. Deze keuze is gemaakt omdat defensie vaak gebruik maakt van deze typen sensoren.

4.1 Demonstratiesysteem

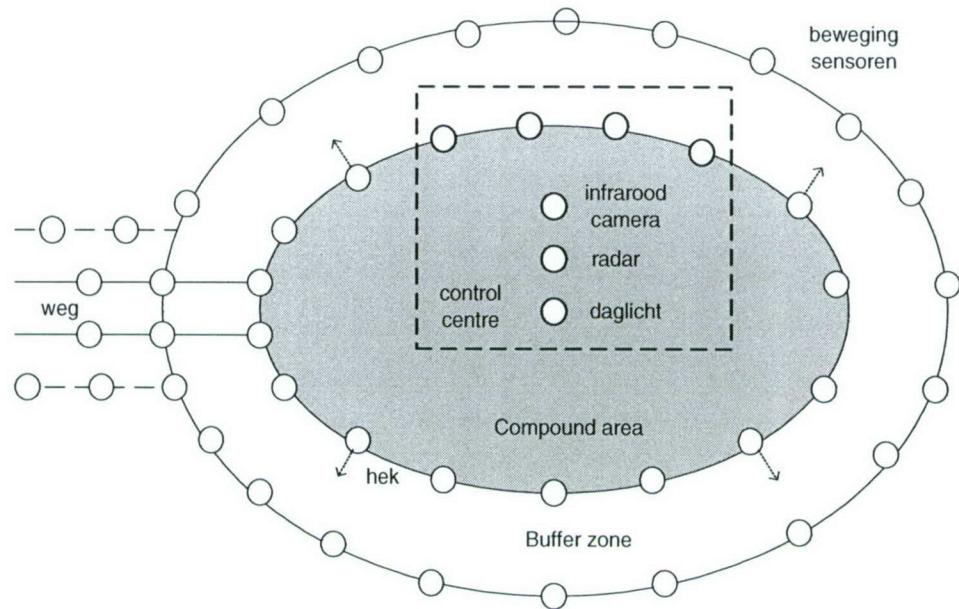
De architectuur van het demonstratiesysteem is getoond in figuur 4.1. De volgende systeemcomponenten voor dit bewakingsysteem kunnen hierin herkend worden:

- een infrarood camera (IR);
- een radarsysteem (Radar);
- een set bewegingsmelders die een autonome sensorgroep vormen (CSD);
- een informatiefusiesysteem (M6T);
- een monitor station (Display Server: DS);
- een controllestation voor diverse instellingen (CS);
- het systeem is optioneel uit te breiden met een Personal Digital Assistant (PDA), die bijvoorbeeld gehanteerd wordt door bewakingpersoneel.



Figuur 4.1 De architectuur van het demonstratie systeem.

De sensoren worden op strategische locaties geplaatst om hun taak goed te kunnen verrichten. Dat betekent dat de bewegingsensoren verdeeld worden in het gebied rond de compound. De radar en infrarood camera worden opgesteld in het centrum van de compound. In figuur 4.2 is dit grafisch weergegeven.



Figuur 4.2 Het praktische demonstratie-scenario. Een compound is volledig omringd door een dubbele ring van sensoren. De infrarood camera en het radarsysteem in de compound worden geïnformeerd door de bewegingsensoren en zullen activiteiten in de gebiedjes rondom de actieve sensoren registreren. De demonstratie gebruikt 4 bewegingsensoren. De M6T fuseert deze data tot tracks. De daglicht camera wordt alleen gebruikt voor visuele inspecties door de operator.

De rest van dit hoofdstuk behandelt de verschillende sensormodules en hun specifieke waarnemingstaak in het compound security demonstratiesysteem. Dit zijn radar, infrarood en een set bewegingsmelders.

4.2 Radar module

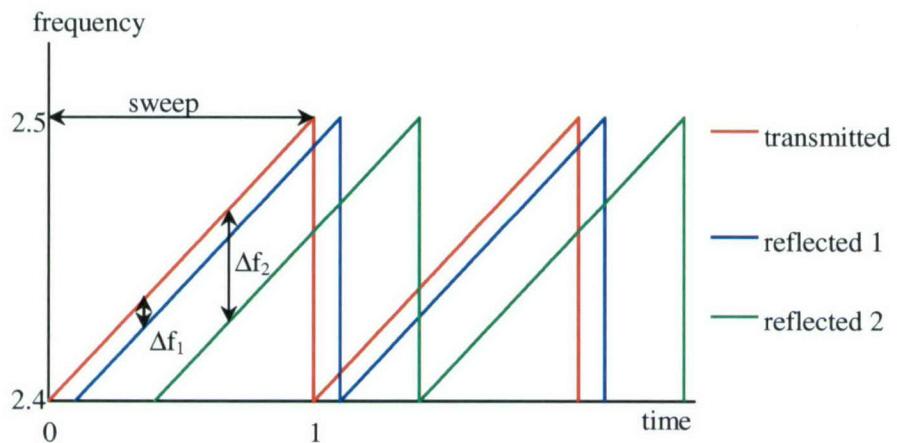
Een radar-sensor is met name geschikt om afstanden tot objecten te meten. Bovendien is het mogelijk om te meten met welke snelheid een obstakel zich beweegt door de afstandsmetingen in de tijd uit te zetten.

Zulke gecombineerde metingen (afstand en snelheid) worden gedaan met een FMCW radar. Een FMCW radar zendt een bepaalde elektromagnetische golf (continuous wave of CW) uit met een variërende frequentie, dit laatste wordt frequentie-modulatie (FM) genoemd.

In principe wordt het FMCW signaal uitgezonden in 'sweeps' van rond de 1 ms. Een sweep bestaat uit een puls waarin de uitgezonden frequentie gestaag wordt verhoogd, uitgaande van de basisfrequentie. De basisfrequentie die voor de demonstratie wordt ingesteld is rond de 2.5 GHz.

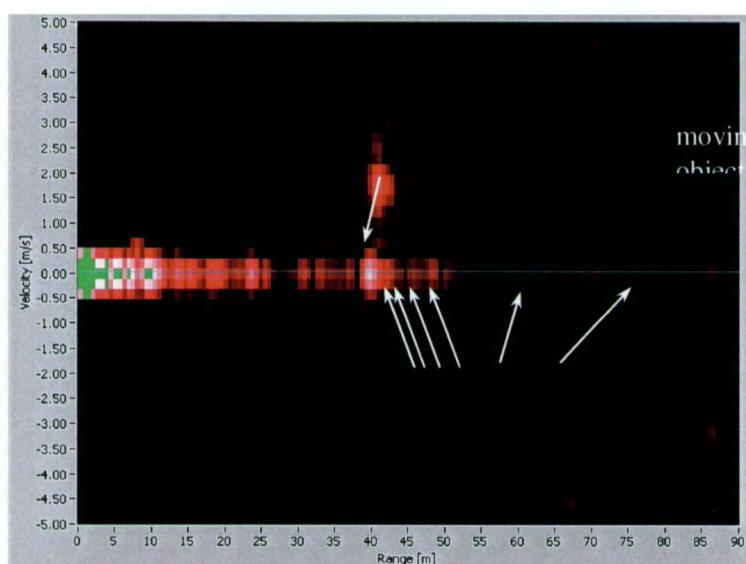
In een sweep wordt bijvoorbeeld de frequentie verhoogd met 250 MHz. Hierbij wordt de uitgezonden frequentie bijvoorbeeld lineair verhoogd van 2.30 GHz tot 2.55 GHz.

Dit signaal wordt in de richting van het object gezonden waarvan de afstand en snelheid tot de radarsensor gemeten moet worden. Het door het object gereflecteerde signaal is een maat voor zijn afstand tot de radar. In figuur 4.3 is dit proces grafisch weergegeven. Het gereflecteerde signaal wordt door de radar gemeten. Het gemeten frequentieverschil Δf geeft het verschil aan tussen de uitgezonden en de ontvangen frequentie. Hoe groter de afstand, hoe groter Δf . De afstand tot het object kan hieruit berekend worden door gebruik te maken van de snelheid van het uitgezonden signaal, dat wil zeggen de lichtsnelheid. Bovendien geeft de intensiteit van het gereflecteerde signaal een indicatie voor de omvang van het object.



Figuur 4.3 FMCW radarsignalen voor afstandsmetingen. Het 'reflected 1' signaal geeft een object op korte afstand aan, het 'reflected 2' signaal toont een object op grotere afstand.

Door het herhaald uitzenden van sweeps in een bekend ritme, kan de snelheid van het object worden bepaald. Dit wordt gedaan door de veranderingen in de Δf metingen te beschouwen. Om dit verder te verduidelijken is in figuur 4.4 een 'range-velocity' diagram getekend. Op de horizontale as staat de range (afstand) en op de verticale as staat de velocity (snelheid). De lijn in het midden represeneert snelheid nul. Dus de meetpunten op deze lijn geven objecten aan die stil staan op de getoonde afstand. Meetpunten boven of onder deze lijn indiceren bewegende objecten.



Figuur 4.4 Range-velocity diagram.

Typische maximale meetdata voor onze radar zijn:

- maximale detectieafstand: 200 m;
- meetresolutie: 60 cm;
- maximale detectiesnelheid: 110 km/hr;
- meetresolutie: 1.8 km/hr.

Voor de demonstratie-opstelling beschreven in dit rapport wordt gebruik gemaakt van het CFAR (Constant False Alarm Rate) algoritme. Dit algoritme maakt gebruik van bovenstaande range-velocity diagrammen.

Het CFAR algoritme genereert een lijst met alle detecties, ook wel contacten genoemd. De metingen worden geclusterd. Dat betekent dat contacten die dicht bij elkaar liggen wat betreft snelheid en afstand, gegroepeerd zijn. Dit is zeer behulpzaam bij het detecteren van loze alarmen. Een loos alarm is een meting van een object dat er in feite niet is. Deze genereren doorgaans kleinere clusters dan in het geval van detecties van echt aanwezige objecten.

4.3 Infrarood module

Voor het opbouwen van een warmtebeeld van de omgeving worden infrarood camera's gebruikt. In het bijzonder mensen en dieren kunnen op deze wijze zeer goed gedetecteerd worden. Met een infrarood camera kan er dus ook 's nachts gedetecteerd worden. In combinatie met een detectie algoritme zoals in de volgende paragraaf is beschreven, is dan een zeer lage vals alarm kans te realiseren.

Een infrarood camera detecteert straling in een bepaald golflengtegebied. De voor deze demonstratie gebruikte camera's zijn een Thermacam of een Radiance 1T. Beide zijn gevoelig in de 3-5 μ golflengteband. De eerste camera is eenvoudig te gebruiken, maar heeft een kleinere field-of-view. De tweede camera beslaat bijna 45 graden, wat in de huidige opstelling een betere dekking geeft van het te bewaken terrein.

Infrarood camera's in de 3-5 μ golflengte band zijn gevoelig voor zowel een deel van de (gereflecteerde) straling van de zon, als voor door objecten uitgezonden warmtestraling. Het temperatuursverschil van een persoon met een niet door zonverhitte achtergrond is daarmee uitstekend te detecteren op de voor deze toepassing relevante afstanden. Ook mist heeft weinig invloed. Alleen zeer hevige regenval of sneeuw zal de prestaties verminderen. Ook kunnen veranderingen in de achtergrond door tijdelijke opwarming door de zon (zeker bij half bewolkt weer) voor alarmen zorgen, die echter lang op een plaats blijven en na tracking eenvoudig te elimineren zijn.

4.3.1 Algoritme

Het te detecteren bewegend object wijkt af van het beeld van de achtergrond. Als dus de mogelijke spreiding van contrasten ten gevolge van normale veranderingen bekend is, kan de kans worden berekend dat een contrast het gevolg is van een object. Door een drempel te leggen op een aan kans gerelateerd contrast, wordt daarmee het aantal te verwachten valse alarmen constant. Dit wordt (net als bij radar) constant false-alarm rate (CFAR) detectie genoemd. Als de spreiding van contrasten een normale verdeling heeft, kan de standaarddeviatie worden gebruikt om een CFAR-drempel te bepalen. Zo is de kans dat het absolute contrast, tengevolge van normaal verdeelde ruis of beweging, boven een drempel van drie maal de standaarddeviatie uitkomt in ons geval

0.27%. Bij een drempel van 6 keer de standaard deviatie is dat al $2 \cdot 10^{-7}\%$. Als de verdeling niet normaal is, zal dit percentage over het algemeen iets groter zijn. Dit is zeker het geval bij bijvoorbeeld bewegende takken.

Een schatting voor de gemiddelde achtergrond en standaarddeviatie kan worden verkregen door de statistiek te bepalen van alle waarden in een beeld. Dit levert echter een slechte schatting op als het beeld niet gelijk is, bijvoorbeeld als er zowel gebouwen, ramen, tegels en planten in beeld zijn. In dat geval kan de statistiek worden bepaald van waarden in een kleiner deel van het beeld. Dit is echter rekenintensief, geeft nog steeds problemen op overgangen van de ene soort achtergrond naar de andere, en kan bovendien de invloed van bewegingen van bomen niet mee nemen. Daarvoor is gedraganalyse in de tijd nodig. Vandaar dat voor het detectiealgoritme de statistiek per pixel wordt bepaald uit meerdere opeenvolgende beelden. Door middel van een cyclische buffer wordt een lopend gemiddelde, en een lopende standaarddeviatie bepaald, waarna per pixel detectie gebeurt door de intensiteit in het huidige beeld te vergelijken met die van het gemiddelde, en een drempel te leggen op een in te stellen aantal keren de lokale standaarddeviatie in de tijd.

Het algoritme levert voor elk gedetecteerde object een ‘blob’ (of cluster) in het infrarood beeld. Deze worden gefilterd om ruis- en andere invloeden te minimaliseren. Van de overgebleven clusters worden de afmeting en locatie in het beeld bepaald, evenals daarvan afgeleide relevante waarden. De resultaten worden in het juiste formaat naar de fusie-tracker (M6T) gezonden.

De output geschiedt volgens het Universal Message Format dat is beschreven in Bijlage A. De bij de alarmen bepaalde kenmerken zijn in eerste instantie in beeldcoördinaten. Deze worden met behulp van tijdens een ijkprocedure bepaalde offsets, en de bekende cameraparameters (zoals field-of-view en aantal pixels) omgerekend naar hoeken in wereldcoördinaten, te weten:

- *Azimuth*: de horizontale hoek van het (gewogen) middelpunt van de detectie, ten opzichte van noord (rechts is positief), in graden.
- *Elevatie*: de verticale hoek van het (gewogen) middelpunt van de detectie, ten opzichte van horizontaal (naar boven is positief), in graden.
- *Width*: de breedte van de *bounding box* rondom de detectie, in mrad.
- *Height*: de hoogte van de *bounding box* rondom de detectie, in mrad.
- *Max*: het maximale binnen de detectie gevonden contrast met de achtergrond.

4.4 CSD module

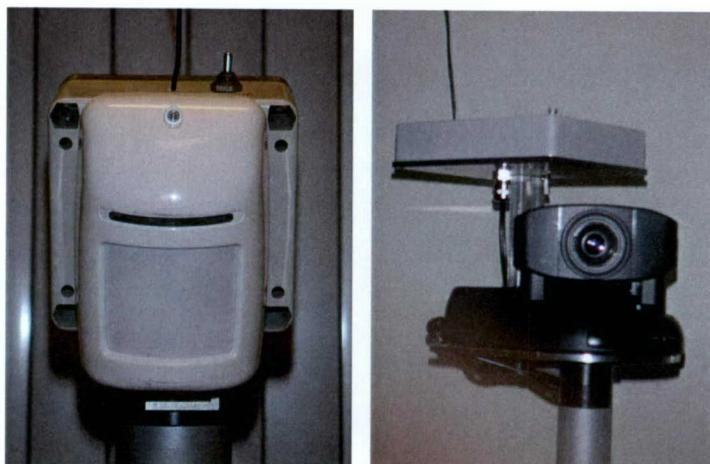
De CSD is een compleet systeem bestaande uit een aantal bewegingssensoren en een camera. In feite is de CSD de voorloper van het bewakingsysteem zoals beschreven in dit rapport. Het grote verschil is dat de CSD gebruik maakt van een enkel type sensor, dat ook nog eens een simpel signaal afgeeft, namelijk een PIR (passive infrared) bewegingsmelder. Het signaal is ‘hoog’ als er beweging wordt geconstateerd, anders ‘laag’.

De bewegingssensoren worden op bekende plaatsen in een veld (bijvoorbeeld rondom de compound) geplaatst. De CSD demonstreert vooral het nut van kleine en goedkope sensoren in een eigen netwerkje. De bevindingen van dit onderzoek dat de CSD beschrijft met uitsluitend de bewegingsensoren is beschreven in [2].

Een belangrijk aspect van de CSD is dat het gebruik maakt van een sensornetwerk. Dat wil zeggen dat zeer kleine en simpele sensoren direct met elkaar communiceren kunnen en dus niet gebruik hoeven te maken van een centrale computer om data uit te wisselen. Het voordeel van deze aanpak is veelvoudig en worden in [2] uitvoerig beschreven. De belangrijkste voordeelen zijn schaalbaarheid, stand-alone operatie en de snelle installeerbaarheid van dit systeem.

De CSD toont een deel van het systeem uit figuur 4.1. Dit systeem bestaat uit vier bewegingsensoren en een centrale die ook een camera kan besturen. Deze zijn op gemakkelijk te plaatsen palen gemonteerd om mobiliteit van dit systeem te benadrukken, zie figuur 4.5.

Voor dit project is de CSD aangepast en maakt nu gebruik van vier TNODes™ (TNO Distributed Embedded Systems). Deze worden in het project SOWnet beschreven, een ander project binnen het programma V219.



Figuur 4.5 (links) De bewegingsensor. Deze bestaat uit een TNODes en een bewegingsmelder als onderdeel van het sensornetwerk. (rechts) De camera is voor observatiedoeleinden als onderdeel van de CSD.

De centrale verwerkingscomputer verzorgt (naast communicatie met de TNODes en de camera) de presentatie van de informatie van het systeem naar de gebruiker. Op het scherm wordt het camerabeeld en de toestanden van de sensoren getoond. In de CSD zijn er vier bewegingsensoren. Deze kunnen vijf verschillende toestanden aannemen, namelijk 'actief', 'beweging', 'beweging is weg', 'sensor niet meer aanwezig' en 'sensor nog niet aanwezig'. Elke toestand wordt met een bepaalde kleurcombinatie gerepresenteerd. Voor de M6T wordt in dit project alleen de melding 'beweging' als contact doorgegeven op het netwerk.

Na een bewegingsmelding van een sensor zal de (pan/tilt/zoom) camera zich zo instellen dat de omgeving van de signalerende sensor te zien is op het scherm om visueel poolshoogte te kunnen nemen. De camera zal altijd de sensor die als laatste een melding geeft in beeld proberen te krijgen. Hiervoor zijn de sensorposities van tevoren in het geheugen van de computer, die bij de camera hoort, opgeslagen. De camera kan dus niet zelf posities van objecten detecteren (zoals de radar en de infrarood camera) en is als zodanig niet opgenomen in de M6T om observaties van verschillende sensoren tot tracks te fuseren.

5 Fusie en Tracking module M6T

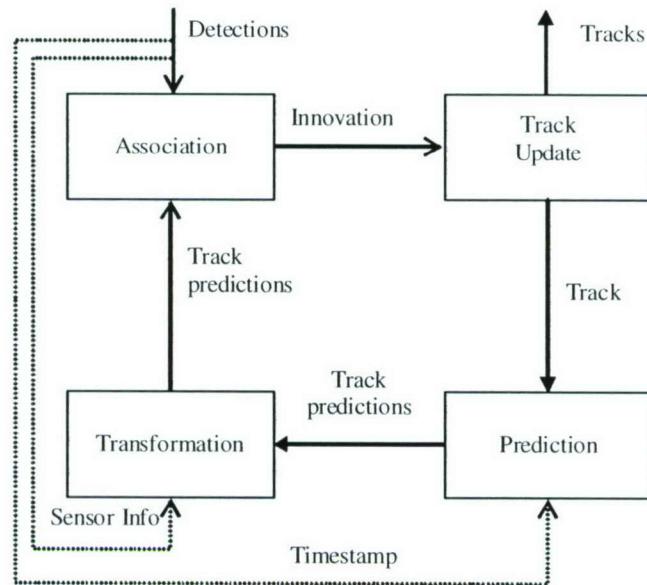
Het tracking algoritme heeft tot doel de metingen van één of meerdere sensoren te associëren met bewegende doelen in de omgeving. De basis hier voor wordt gevormd door een extended Kalman filter dat gebruik maakt van meerdere hypotheses om contacten (detecties) met tracks te associëren.

Op basis van een serie contacten geassocieerd met een doel wordt een schatting berekend voor de werkelijke beweging van het doel. Een reeks van deze toestandsschattingen vormt een track. De toestandsvariabelen die geschat kunnen worden door het tracking-proces hangen af van de beschikbare sensordata.

De bewegingsmelders, de infraroodcamera en de radar geven allemaal series van detecties. De sensoren leveren daarmee verschillende parameters van de gedetecteerde doelen: de radar geeft afstand en radiale snelheid, de IR camera geeft azimut en elevatie, en de bewegingsmelders geven enkel de aanwezigheid van een doel binnen het meetbereik. Dit vormt de input van het tracking algoritme, en deze associeert de detecties tot tracks van één of meerdere doelen. Op deze wijze wordt de sensorinformatie gefuseerd, en deze inkapseling van de datafusie in het tracking-algoritme wordt dan ook 'Fuse while track' genoemd.

De geometrische en dynamische informatie gegeven door de detecties wordt meestal gegeven in het coördinaatsysteem van de sensor (de meetruimte). De tracks zijn gegeven in een cartesisch of geodetisch systeem (toestandsruimte) dat geschikt is om een sensoronafhankelijk omgevingsbeeld op te bouwen. Bij meerdere sensoren zal de toestandsruimte daarom verschillen van de afzonderlijke meetruimtes.

Een overzicht van het fusie en tracking-proces is gegeven in figuur 5.1. Op het moment dat er een detectie binnenkomt wordt op basis van het tijdstip waarop de detectie plaats vond (timestap) en de laatst geschatte toestand van de track (track update) een voorspelling (prediction) gedaan waar het object zich op het tijdstip van detectie bevindt. Deze voorspelling wordt getransformeerd naar de specifieke meetruimte van de sensor waarmee de detectie gemeten is. Op basis hiervan vind associatie van de detectie aan de track plaats. Het verschil tussen de voorspelde en de gemeten toestand wordt vervolgens gebruikt om met behulp van een Kalman filter een nieuwe toestandschatting te maken.



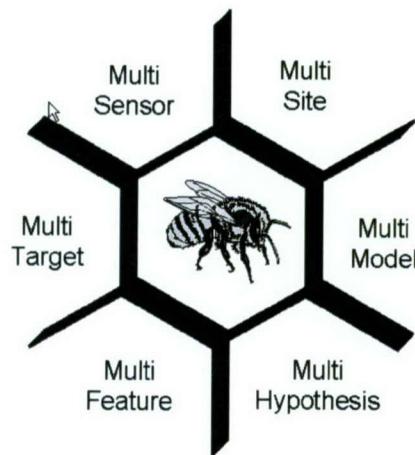
Figuur 5.1 Overzicht van het tracking-proces met contacten die afkomstig zijn van verschillende sensoren.

De associatie van detecties aan een variabel aantal tracks kan op twee manieren gedaan worden:

- ofwel met een *nearest-neighbour* algoritme waarbij elke detectie afzonderlijk geassocieerd met het track dat, gewogen met de meet- en tracknauwkeurigheid, het dichtst bij de detectie ligt;
- of door middel van *Multi Hypothese Tracking* (MHT), hierbij worden verschillende detectie-track associatiehypoteses (inclusief loze en gemiste detecties) met bijbehorende waarschijnlijkheden bijgehouden.

In gevallen waar meerdere doelen ambigue metingen opleveren die slechts opgelost kunnen worden door detecties van meerdere sensoren en meerdere tijdstippen te combineren, zal de eerste methode niet toereikend zijn. De meerwaarde van MHT bestaat uit het feit dat meerdere associatiehypoteses behouden worden totdat op basis van latere detecties een ondubbelzinnige associatie gemaakt kan worden. De toestand van het doel kan ook bijgehouden worden bij gemiste detecties, zodat het doel gevuld kan worden voor zolang deze zich binnen het meetdomein van de sensoren bevindt.

De verschillende sensoren leveren complementaire metingen (de radar levert afstand en snelheid, de camera azimut en elevatie) en detecties worden zowel tegelijkertijd als asynchroon door de sensoren gegenereerd. Hierdoor is de MHT aanpak beter geschikt om gebruik te maken van de voordelen van een multi-sensor systeem. Dit wordt deels veroorzaakt doordat voor kortere tijdsintervallen tussen verschillende detecties de associatiemogelijkheden sterker gecorreleerd zijn. Om de waarschijnlijkheden van de associatiehypoteses voor een nieuwe detectie te berekenen moet de kans bekend zijn dat een doel door geen enkele sensor gedetecteerd is in het interval tussen deze en de voorlaatste detectie van dit doel. Nauwkeurige kennis van de *a priori* detectiekansdichtheden van de sensoren is dus nodig om de kans op een gemiste detectie te kunnen berekenen. De dichtheid van loze detecties kan geschat worden uit metingen waarbij zich geen doelen in het meetdomein bevinden.

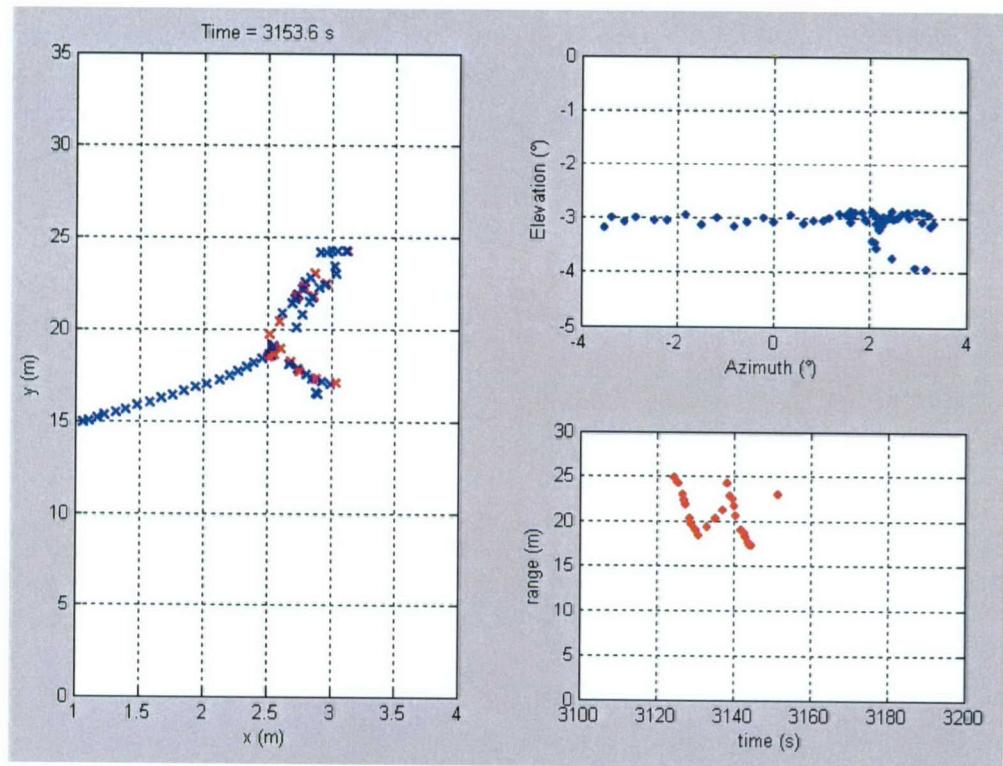


Figuur 5.2 Grafische voorstelling van de M6T sensor fusie en tracking module.

5.1 Resultaten

De demonstratie-opstelling bestond uit de CSD met vier bewegingsensoren, de radar en de infrarood camera. De CSD-sensoren werden gebruikt om de andere twee typen sensoren te 'triggeren' dat er beweging waargenomen was in een bepaald gebied op het veld rond de compound. Daarna stelden de infrarood-camera en radar zich zo in dat ze dat gebied konden waarnemen. Vervolgens werd de informatie van die twee sensoren gecombineerd tot tracks met behulp van de M6T fusie en tracker module. Het resultaat is getoond in figuur 5.2. Aan de linkerkant van deze figuur staat de locatie van de waargenomen objecten (twee personen die in het gebied liepen) in x,y positie-coördinaten. De positiecoördinaten werden over een periode van 22 seconden berekend, gebruik maken van de waarnemingen van de beide sensoren. Rechtsboven in deze figuur staan de waarnemingen van de infrarood camera, terwijl rechtsonder de metingen van de radar weergegeven zijn.

Dit resultaat toont de principewerking van de tracker-module en laat zien hoe data van totaal verschillende sensoren gecombineerd kan worden tot informatie die gemakkelijk interpreteerbaar is door een menselijke gebruiker.



Figuur 5.2 Gecombineerde track (links) van twee sensoren, infrarood (rechtsboven) en radar (rechtsonder). Deze track is berekend door de M6T en geeft de locatie van het waargenomen object in x,y-coördinaten.

6 Conclusie

Het Testbed is gereed voor gebruik. De omgeving kan gebruikt worden voor het testen en evalueren van multi-device systemen, bijvoorbeeld in het kader van NEC. Er is aangetoond dat data van verschillende sensoren, kunnen worden samengevoegd tot bruikbare informatie. Als demonstratiesysteem is er gekozen voor het detecteren en volgen van bewegende mensen waarbij metingen van verschillende sensoren in het volgproces worden gecombineerd.

Doordat elk device gebruik maakt van DeviceML kunnen we elk apparaat (device) op een 'hoog' systeemniveau op een gestandaardiseerde wijze omschrijven. Het is gebleken dat deze werkwijze zeer geschikt is om de verschillende apparaten op gemakkelijke wijze met elkaar in verbinding te brengen.

Tijdens dit project is gebleken dat informatie-uitwisseling tussen verschillende systemen in een genetwerkte omgeving geenszins triviaal is. De uitdaging zal blijven zitten in het definiëren van de juiste interfaces die aan de ene kant generiek en flexibel zijn en aan de andere kant specifiek en applicatieafhankelijk zijn.

7 Referenties

- [1] Janssen, J.A.A.J. et al.; *Definitie Testbed Omgeving*; TNO rapport FEL-03-A283; September 2003.
- [2] Dijk, G. van et. al.; *Compound Security Demonstrator*; TNO rapport FEL-04-B065; September 2003.
- [3] Botts, M. Reichardt, M.; *Sensor Web Enablement White Paper*; Open GIS Consortium; Wayland, V.S..
- [4] Open GIS Consortium; <http://www.opengis.org>.
- [5] Open GIS Consortium Inc.; *Sensor Model Language (SensorML) for In-situ and Remote Sensors*; Open GIS Consortium Inc.; OGC 02-026r4, version 0.7; December 2002.
- [6] Open GIS Consortium Inc.; *Observations and Measurements*; Open GIS Consortium Inc.; OGC 03-022r3, version 0.9.2; April 2002.
- [7] <http://hdf.ncsa.uiuc.edu/>.
- [8] Janssen, J.A.A.J. en Maris, M.G. *Self-Configurable Distributed Control Networks on Naval Ships*, In proceedings of SCSS 2003.

8 Ondertekening

Den Haag, mei 2006

TNO Defensie en Veiligheid



dr. A. Verweij
Afdelingshoofd



dr. L.J.H.M. Kester
Auteur

A Universal Contact Message format

This appendix describes a universal contact message to be used between a plot extraction algorithm and a tracker. A universal contact message improves the interchangeability of trackers and detection algorithms. This contact message is setup to be easily extended with additional sensors and sensor parameters. Additionally a file header is specified.

Message format

Each message with contacts has the following structure:

```
<big/little endian id> <sensor id> <message id>
<header format id> <number of contacts> <header parameter 1> ... <header parameter n>
<contact format id> <measurement parameter 1> ... <measurement parameter n>
...
<contact format id> <measurement parameter 1> ... <measurement parameter n>
```

A binary format for the fields is chosen since this decreases the message length compared to an ASCII message. For user readability the different fields are split into different lines, in the actual message all fields are concatenated. The parameters mentioned in the header line apply to all detections (for example timestamp or surrounding temperature) whereas the parameters in the contact lines only apply to that contact. The number of parameters in the header line and contact lines can be unlimitedly extended to the required number.

The fields are described as:

field	format	description
big/little endian identifier	U4 ¹	always contains number 0x12345678
sensor id	U4	unique sensor number for specific measurement setup
message id	U4	serial number for blocks of contacts from one sensor, for each sensor this number starts with 1
number of contacts	U4	number of contacts in message
header format id	U4	header format number
contact format id	U4	contact format number
contact format id	U4	contact format number

¹ Un means unsigned n bytes integer

Fn means n bytes floating point number

In means signed n bytes integer

Sn means n bytes string

Example

Two contacts from a radar with sensor id 1 need to be passed to the tracker. Both contacts have the same timestamp of 3.04 s (F4). The first contact is a cluster of 12 detections and contains both range of 4.6 m (F4) and velocity of 3.42 m/s (F4) information. The second contact only contains range information of 10.3 m (F4). Since the beginning of the measurement this is message 34. This is written in the universal contact message, using specifications mentioned below, like:

12345678 1 34 1 2 3.04 12 1 4.6 3.42 2 10.3

In more readable form this looks like:

```
12345678 1 34
1 2 3.04 12
1 4.6 3.42
2 10.3
```

Everybody that will use this format will have to assign a sensor id to his or her sensors. This sensor id can differ for different measurement setups.

Below a sample specification is given.

Sensor 1: 2.4 GHz FMCW radar

Header format id 1: number of contacts in message (U4), timestamp since beginning measurement [s] (F4)

Contact format id 1: range [m] (F4), velocity [m/s] (F4), Amplitude (F4), number of detections in contact (U4)

Contact format id 2: range [m] (F4)

Sensor 2: Passive Radar

Header format id 1: number of contacts in message (U4), GPS timestamp [F4] (#seconds since midnight)

Header format id 2: number of contacts in message (U4)

Contact format id 1: range [m] (F4), doppler [Hz] (F4)

Contact format id 2: range [m] (F4), doppler [Hz] (F4), Azimuth [°] (F4), Amplitude [a] (F4)

Contact format id 3: range [m] (F4), doppler [Hz] (F4), Azimuth [°] (F4), Amplitude [?] (F4), TrackID [-] (U4), Latitude (WGS84) [°] (F4), Longitude (WGS84) [°] (F4), Altitude [m] (F4), Mode 3/A [-] (S4)

Contact format id 4: time [s] (F4), range [m] (F4), doppler [Hz] (F4)

ONGERUBRICEERD

REPORT DOCUMENTATION PAGE (MOD-NL)

1. DEFENCE REPORT NO (MOD-NL)	2. RECIPIENT'S ACCESSION NO	3. PERFORMING ORGANIZATION REPORT NO
TD2005-0377	-	TNO-DV1 2005 A153
4. PROJECT/TASK/WORK UNIT NO	5. CONTRACT NO	6. REPORT DATE
015.33721	-	May 2006
7. NUMBER OF PAGES	8. NUMBER OF REFERENCES	9. TYPE OF REPORT AND DATES COVERED
34 (incl 1 appendix, excl RDP & distribution list)	8	Final
10. TITLE AND SUBTITLE		
Testbed environment for distributed observation (Testbed omgeving voor gedistribueerde waarneming)		
11. AUTHOR(S)		
Dr L.J.H.M. Kester Dr M.G. Maris		
12. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)		
TNO Defence, Security and Safety, P.O. Box 96864, 2509 JG The Hague, The Netherlands Oude Waalsdorperweg 63, The Hague, The Netherlands		
13. SPONSORING AGENCY NAME(S) AND ADDRESS(ES)		
Royal Netherlands Navy		
14. SUPPLEMENTARY NOTES		
The classification designation Ongerubriceerd is equivalent to Unclassified, Stg. Confidentieel is equivalent to Confidential and Stg. Geheim is equivalent to Secret.		
15. ABSTRACT (MAXIMUM 200 WORDS (1044 BYTE))		
In the future, military operations will have a network-centric character. This means that many heterogeneous devices, such as sensors and actuators are deployed. The information coming from those devices must be fused such that an integrated system results. Such devices may be mounted on unmanned platforms or as standalone systems. This report describes a testbed environment to integrate, test and evaluate such cooperating systems.		
16. DESCRIPTORS		IDENTIFIERS
Distributed Systems Model Tests Multi Sensors Platforms Sensors		
17a.SECURITY CLASSIFICATION (OF REPORT)	17b.SECURITY CLASSIFICATION (OF PAGE)	17c.SECURITY CLASSIFICATION (OF ABSTRACT)
Ongerubriceerd	Ongerubriceerd	Ongerubriceerd
18. DISTRIBUTION AVAILABILITY STATEMENT		17d.SECURITY CLASSIFICATION (OF TITLES)
Unlimited		Ongerubriceerd

ONGERUBRICEERD

Distributielijst

Onderstaande instanties/personen ontvangen een volledig exemplaar van het rapport.

- 1 DMO/SC-DR&D
standaard inclusief digitale versie bijgeleverd op cd-rom
- 2 DMO/DR&D/Kennistransfer
- 3 DMO/Land/CIS
- 4 DMO/Zee/S&W/Bureau Sensoren
- 5 Programmabegeleider DMO, drs. W. Pelt.
- 6 OCT Genie, Th.G.M. van Wijk
- 7 CTM, ir. A. van Bladel
- 8/10 Bibliotheek KMA
- 11 TNO Defensie en Veiligheid, vestiging Den Haag,
Manager Waarnemingssystemen (operaties), dr. M.W. Leeuw
- 12 Programmaleider TNO Defensie en Veiligheid, ing. J.C.P. Bol
- 13 TNO Defensie en Veiligheid, vestiging Rijswijk,
Vormgeving en Tekstverwerking, (daarna reserve archief)
- 14 TNO Defensie en Veiligheid, vestiging Den Haag,
Archief
- 15/17 TNO Defensie en Veiligheid, vestiging Den Haag,
Business Unit Waarnemingssystemen
dr. L.J.H.M. Kester
dr. M.G. Maris
dr. J.A.A.J. Janssen
- @ TNO Defensie en Veiligheid, vestiging Rijswijk,
Marketing en Communicatie (digitale versie via Archief)

Onderstaande instanties/personen ontvangen het managementuittreksel en de distributielijst van het rapport.

- 4 ex. DMO/SC-DR&D
- 1 ex. DMO/ressort Zeesystemen
- 1 ex. DMO/ressort Landsystemen
- 1 ex. DMO/ressort Luchtsystemen
- 2 ex. BS/DS/DOBBP/SCOB
- 1 ex. MIVD/AAR/BMT
- 1 ex. Staf CZSK
- 1 ex. Staf CLAS
- 1 ex. Staf CLSK
- 1 ex. Staf KMar
- 1 ex. TNO Defensie en Veiligheid, Algemeen Directeur, ir. P.A.O.G. Korting
- 1 ex. TNO Defensie en Veiligheid, Directie Directeur Operaties, ir. C. Eberwijn
- 1 ex. TNO Defensie en Veiligheid, Directie Directeur Kennis, prof. dr. P. Werkhoven
- 1 ex. TNO Defensie en Veiligheid, Directie Directeur Markt, G.D. Klein Baltink
- 1 ex. TNO Defensie en Veiligheid, vestiging Den Haag, Manager Beleidsstudies Operationele Analyse & Informatie Voorziening (operaties), drs. T. de Groot
- 1 ex. TNO Defensie en Veiligheid, vestiging Rijswijk, daarna reserve Manager Bescherming, Munitie en Wapens (operaties), ir. P.J.M. Elands
- 1 ex. TNO Defensie en Veiligheid, vestiging Rijswijk, Manager BC Bescherming (operaties), ir. R.J.A. Kersten
- 1 ex. TNO Defensie en Veiligheid, vestiging Soesterberg, Manager Human Factors (operaties), drs. H.J. Vink

